Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

98. (Currently Amended) A computer-readable medium comprising a program for encrypting a private key used in cryptography, wherein the private key conforms to a predetermined key format, the program being executable on a computer to carry out the steps of:

dividing an exponent of the private key into a most significant portion and a least significant portion;

encrypting the least significant portion using a secret known to a user associated with the private key; and

combining the most significant portion, without encryption, and the encrypted version of the least significant portion to form a storable private key sequence, the storable private key sequence being such that a decryption of the storable private key sequence using a proposed secret other than the secret known to the user results in a decrypted pseudo-key, wherein a pseudo-key is a key that conforms to the predetermined key format but does not match the private key and wherein the number of proposed secrets that lead to a pseudo-key is larger than a security threshold~~,~~; and

storing the ~~combined portions~~ storable private key sequence as the encrypted private key.

99. (new) The computer-readable medium of claim 98, wherein the security threshold is determined by a secured resource that validates the private key and disables at least usage of the private key after receipt of the security threshold number of pseudo-keys.

100. (new) The computer-readable medium of claim 98, wherein the secret known to the user is a personal identification number (PIN) selected from a PIN space and more than the security threshold number of PINs in the PIN space result in pseudo-keys.

101. (new) The computer-readable medium of claim 98, wherein the predetermined key format is a format wherein a key exponent is less than a maximum valid exponent.

102. (new) The computer-readable medium of claim 101, wherein the program is further configured to carry out the steps of:

selecting random numbers k and m, where m is a number between d, the exponent of the private key, and n, the modulus of the private key.

computing a sum d+km from d, k and m;

encrypting the sum d+km using the secret known to the user associated with the private key, to form an encrypted sum;

storing the random number m and the encrypted sum as the encrypted private key, thereby generating a value that is less than the modulus of the private key whether decrypted with the secret known to the user or with a proposed secret other than the secret known to the user.

103. (new) The computer-readable medium of claim 102, wherein k is a 64-bit value.

104. (new) A computer-readable medium comprising a program for encrypting a private key used in cryptography, wherein the private key conforms to a predetermined key format, the program being executable on a computer to carry out the steps of:

dividing the private key into a first portion and a second portion;

encrypting the second portion using a secret known to a user associated with the private key to form an encrypted second portion such that a substitution of an incorrectly decrypted encrypted second portion for the correctly decrypted encrypted second portion results, for at least some proposed secrets other than the secret known to the user, in a pseudo-key that conforms to the predetermined key format but is different from the private key; and combining the first portion, without encryption, and the encrypted second portion to form a storable private key sequence, the storable private key sequence being such that a decryption of the storable private key sequence using at least some proposed secrets other than the secret known to the user results in a decrypted pseudo-key, wherein the number of proposed secrets that lead to a pseudo-key is larger than a security threshold; and

storing the storable private key sequence as the encrypted private key.

105. (new) The computer-readable medium of claim 104, wherein the security threshold is determined by a secured resource that validates the private key and disables at least usage of the private key after receipt of the security threshold number of pseudo-keys.

106. (new) The computer-readable medium of claim 104, wherein the secret known to the user is a personal identification number (PIN) selected from a PIN space and more than the security threshold number of PINs in the PIN space result in pseudo-keys.

107. (new) The computer-readable medium of claim 104, wherein the predetermined key format is a format wherein a key exponent is less than a maximum valid exponent.

108. (new) The computer-readable medium of claim 107, wherein the program is further configured to carry out the steps of:

selecting random numbers k and m, where m is a number between d, the exponent of the private key, and n, the modulus of the private key.

computing a sum d+km from d, k and m;

encrypting the sum d+km using the secret known to the user associated with the private key, to form an encrypted sum;

storing the random number m and the encrypted sum as the encrypted private key, thereby generating a value that is less than the modulus of the private key whether decrypted with the secret known to the user or with a proposed secret other than the secret known to the user.

109. (new) The computer-readable medium of claim 108, wherein k is a 64-bit value.